PHILIPPINES

CHECK AGAINST DELIVERY

INTERVENTION

On How International law applies to the use of information and communications technologies by States

Delivered by

by Ms. Kristine Margret M. Malang
Alternate Representative
Permanent Mission of the Republic of the Philippines
to the United Nations in New York

First Substantive Session of the Open-ended Working Group (OEWG) on security of and in the use information and communications technologies (ICT) 2021-2025

UN General Assembly Hall, United Nations Headquarters, New York
15 December 2021, 03:00 p.m.

Mr. Chair,

At this juncture, on the applicability of international law in cybersecurity issues, the Philippines would like to highlight the following points and raise some issues that we need to take into account as we delve into this subject further:

1. We already have consensus on the applicability of international law to cross-border cyberoperations but there is a need to further study the precise application and interpretation of many of these international law principles and the rules that govern them.

2. We should also balance the applicability of international law in cyberoperations so as not to unduly restrain "peaceful" activities in cyberspace by States and non-State actors.

3. International law provides a number of legal bases on how States should lawfully respond to harmful/malicious cyberoperations during peacetime. The OEWG may further discuss certain aspects such as:

    a. **Self-defense** -This is anchored on Article 51 of the UN Charter which provides that "nothing in the present Charter shall impair the inherent right of individual or collective self-defense if an armed attack occurs against a Member of the UN…" This response requires, as a condition precedent of the right to engage in self-defense, that an

"armed attack" is present. What needs to be discussed thoroughly by the OEWG is the concept of what constitutes an "armed attack" in the context of cyberoperations to justify resort to self-defense? Does it require a resulting harm? What is the threshold of severity for the cyberoperation to amount to an "armed attack"?

b. Another aspect which needs to be considered is the **nature of cyberoperations**. We know that the general rule in international law is that a State is only entitled to respond in self-defense if an armed attack is either imminent or ongoing. However, malicious cyberoperations, by its very nature, may be executed in seconds or even less, and it leaves the target State with no warning or time to respond to the cyberattack. Will highly reliable intelligence that an armed attack will be launched against a State be sufficient to justify resort to self-defense? How about a situation where a victim State reasonably concludes that further cyberattacks will be launched against it?

c. We also need to consider – **countermeasures**.

Countermeasures are responses by a State to the unlawful cyberoperations of, or attributable to, another State. The purpose is to cause the responsible State to desist in malicious cyberoperations against the victim State. The question, however is, what if the identity of the actor causing the malicious cyberoperation is uncertain? And how certain must a State be in attributing a malicious cyberoperation before launching a countermeasure? If the cyberoperation is indeed attributable to a State, countermeasures are available as a remedy when the responsible State is in breach of an international legal obligation such as respecting the sovereignty of the victim State. By permanently affecting the functionality of cyber infrastructure there is a breach of sovereignty and therefore, the victim State may launch countermeasures against the responsible State. But how about in situations where the damage is not of a permanent nature or the damage is not grave enough but has somehow affected/altered a State's critical infrastructure?

Mr. Chair,

In our succeeding meetings and sessions among members and stakeholders, the Philippines looks forward to threshing out these issues with the view of forming consensus on how existing international law may prove to be responsive and how other proposals for binding instruments would prove to be necessary to address cybersecurity threats and issues.

Thank you, Mr. Chair.